日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: １９９９年　６月　２日

出願番号
Application Number: 平成１１年特許願第１５４６５７号

出願人
Applicant (s): 株式会社日立製作所

U.S. Appln. Filed 6-2-00
Inventor: T. Yazaki et al
Mathingly, Stanger & Malur
M17-200

２０００年　５月１２日

特許庁長官
Commissioner,
Patent Office 近藤隆彦

出証番号　出証特２０００－３０３３２７０

【書類名】　特許願

【整理番号】　H99013251A

【提出日】　平成11年 6月 2日

【あて先】　特許庁長官　殿

【国際特許分類】　H04L 12/56

【発明者】

【住所又は居所】　東京都国分寺市東恋ケ窪一丁目２８０番地
株式会社日立製作所中央研究所内

【氏名】　矢崎　武己

【発明者】

【住所又は居所】　東京都国分寺市東恋ケ窪一丁目２８０番地
株式会社日立製作所中央研究所内

【氏名】　相本　毅

【特許出願人】

【識別番号】　000005108

【氏名又は名称】　株式会社日立製作所

【代理人】

【識別番号】　100075096

【弁理士】

【氏名又は名称】　作田　康夫

【電話番号】　03-3212-1111

【手数料の表示】

【予納台帳番号】　013088

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　帯域監視方法および装置

【特許請求の範囲】

【請求項１】

特定種類のパケットを前記特定種類以外のパケットよりも優先して送信するネットワークにおける帯域監視方法であって、

前記ネットワークにパケットが流入した場合、前記パケットが前記パケットの送信元との契約されている契約帯域に違反していないかを監視し、

前記パケットが前記特定種類のパケットであるか否かを判断し、

前記パケットが契約帯域に違反しておらず、かつ、前記特定種類のパケットでない場合に、前記パケットを前記特定種類のパケットとして送信することを特徴とする帯域監視方法。

【請求項２】

前記パケットは、ヘッダを有しており、前記ヘッダ内の値に応じて前記パケットが前記特定の種類のパケットであるか否かを判断することを特徴とする請求項１に記載の帯域監視方法。

【請求項３】

前記ヘッダ内の値が、前記特定の種類のパケットを示す値でない場合に、前記ヘッダ内の値を前記特定の種類のパケットを示す値に再設定することを特徴とする請求項２に記載の帯域監視方法。

【請求項４】

前記ヘッダは優先度フィールドを有しおり、前記優先度フィールドの値により前記パケットが前記特定の種類のパケットであるか否かを判断することを特徴とする請求項２又は請求項３の何れかに記載の帯域監視方法。

【請求項５】

特定種類のパケットを前記特定種類以外のパケットよりも優先して送信するネットワークにおける帯域監視方法であって、

前記ネットワークにパケットが流入した場合、前記パケットが前記パケットの送信元との契約されている契約帯域に違反していないかを監視し、

前記パケットが前記特定種類のパケットであるか否かを判断し、

前記パケットの送信元が使用している帯域が前記契約帯域より小さい第１の帯域以下であり、かつ、前記パケットが前記特定種類のパケットでない場合に、前記パケットを前記特定種類のパケットとして送信することを特徴とする帯域監視方法。

【請求項６】

前記パケットの送信元が使用している帯域が前記第１の帯域を越えており、かつ、前記パケットが前記特定種類のパケットでない場合に、前記パケットは前記特定種類以外のパケットとして送信することを特徴とする請求項５に記載の帯域監視方法。

【請求項７】

前記パケットの送信元が使用している帯域が前記契約帯域を越えており、かつ、前記パケットが前記特定種類のパケットである場合に、前記パケットを前記特定種類以外のパケットとして送信することを特徴とする帯域監視方法。

【請求項８】

前記パケットが特定種類以外のパケットである場合には、第１のバケツの深さを有するリーキーバケットアルゴリズムを使用し、前記パケットが特定種類のパケットである場合には、前記第１のバケツの深さとは異なる第２のバケツの深さを有するリーキーバケットアルゴリズムを使用することにより、前記パケットが前記パケットの送信元との契約されている契約帯域に違反していないかを監視することを特徴とする請求項５乃至７の何れかに記載の帯域監視方法。

【請求項９】

ネットワークに流入するパケットの帯域を監視する帯域監視装置であって、

入力パケットのアドレス情報、用途を識別する情報又は前記ネットワーク内の優先度を識別する情報であるネットワーク優先度のうち少なくとも一つの情報からパケットの一連のフロー(流れ)を検出して、前記フローの識別子であるフロー識別子と優先度であるフロー優先度を判定するフロー検出手段と、帯域監視のための制御情報である帯域監視制御情報と複数の前記ネットワーク優先度から構成されるエントリを一つあるいは複数所持する帯域監視テーブルと、前記フロー識

別子に対応するエントリを帯域監視テーブルから読み出す帯域監視テーブル制御手段と、前記フロー優先度と前記帯域監視テーブル制御手段が読み出したエントリ内の帯域監視制御情報と現時刻を表すタイマーの値に基づいて前記入力パケットの遵守・違反の判定を行う監視結果判定手段と、前記監視結果判定手段の判定結果と前記帯域監視テーブル制御手段が読み出した複数のネットワーク優先度から前記入力パケットのネットワーク優先度を判定する優先度判定手段することを特徴とする帯域監視装置。

【請求項１０】

ネットワークに流入するパケットの帯域を監視する帯域監視装置であって、入力パケットのコネクション情報から前記コネクションの優先度であるコネクション優先度を判定するコネクション優先度判定手段と、帯域監視のための制御情報である帯域監視制御情報と複数の前記ネットワーク内の優先度を識別する情報であるネットワーク優先度から構成されるエントリを一つあるいは複数所持する帯域監視テーブルと、前記コネクション識別子に対応するエントリを帯域監視テーブルから読み出す帯域監視テーブル制御手段と、前記コネクション優先度と前記帯域監視テーブル制御手段が読み出したエントリ内の帯域監視制御情報と現時刻を表すタイマーの値に基づいて前記入力パケットの遵守・違反の判定を行う監視結果判定手段と、前記監視結果判定手段の判定結果と前記帯域監視テーブル制御手段が読み出した複数のネットワーク優先度から前記入力パケットのネットワーク優先度を判定する優先度判定手段することを特徴とする帯域監視装置。

【請求項１１】

監視結果判定手段の前記帯域監視のアルゴリズムとしてバケツの深さを複数有するリーキーバケットアルゴリズムを使用し、前記帯域監視制御情報として優先パケット用のバケツの深さと優先パケット以外のパケット用のバケツの深さを所持することを特徴とする請求項９又は請求項１０の何れかに記載の帯域監視装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、ネットワークに流入するパケットの帯域を監視する帯域監視方法および帯域監視装置に関する。

【０００２】

【従来の技術】

インターネットユーザの増加に伴い、インターネットを流れるトラヒック（パケット）が急増している。インターネットで用いられているパケット型通信方式では、多数のユーザからのパケットを、同じ回線を用いて送信できる。そのため、帯域あたりのコストを低く抑えることが出来る。このパケット型通信方式の低コスト性の為、従来、専用の網で実現していた電話網や企業網をインターネットで統合して、通信コストの低減を実現しようという動きが出てきた。これらを統合するためには、従来の電話網や企業網が実現していた低遅延時間や低廃棄率等の通信品質（QoS：Quality of Service）を実現する必要がある。

【０００３】

QoSに関する従来技術としては、例えば、IETF(Internet Engineering Task Force)のRFC2475に記されているDiffserv(Differentiated Service)（以下「従来技術1」という。）がある。従来技術1では、サービスを提供するネットワークの入口において、トラヒック(パケット)はTCP/IPヘッダ内の送信元・宛先IPアドレス、送信元・宛先ポート番号、プロトコル等によりクラス分けされ、転送動作が割り当てられると記載されている。さらに、ネットワーク内において、パケットはヘッダ内のDSCP(Differentiated Service Code Point)に関連付けられた転送動作に基づき転送されると記載されている。ネットワークの入口のノードが低遅延時間や低廃棄率が必要なパケットに優先的に転送される転送動作を割り付けて、ネットワーク内のノードが前記パケットを優先的に転送することにより、前記パケットの低遅延時間や低廃棄率を実現することができる。なお、本願では優先的に転送される転送動作が割り当てられるパケットを優先パケットと、それ以外のパケットを非優先パケットと呼ぶ。

【０００４】

QoSを実現するネットワークでは、ユーザとの間に、優先パケットの帯域の契約が行われる。ネットワークの入口のノードは帯域監視機能を有し、前記帯域で監視(帯域監視)する。帯域監視機能に関しては例えば前記従来技術1に記載されている。従来技術1では、ユーザとネットワークとの間で、転送動作の判定ルール(音声パケットは優先等)や帯域等の契約(TCA: Traffic Conditioning Agreement)が行われ、ネットワークの入口のノードはTCAを満足する様にパケットを廃棄したりDSCPを変更したりすると記載されている。この帯域監視機能をネットワークの入口のノードが所持することにより、１ユーザの大量の優先パケットがネットワーク内に流入すること防止し、他ユーザの優先パケットのQoSを実現する。

【０００５】

帯域監視機能はATM(Asynchronous Transfer Mode)で一般的である。ATMにおける帯域監視に関しては、例えば、The ATM Forum Specification version 4.0の4.5章(以下「従来技術２」という。)に記載されている。従来技術２に記載されているVBR (Variable Bit Rate)サービスでは、ユーザーネットワーク間で最大帯域(PCR: Peak Cell Rate)および平均帯域(SCR: Sustainable Cell Rate)が契約される。ユーザはセルヘッダ内のセル廃棄の優先度を表すCLP(Cell Loss Priority)を重要度に応じて優先(＝0：廃棄が発生しにくい)または非優先(＝1：廃棄が発生し易い)として送出する。CLPが0のパケットを平均帯域で監視し、違反パケットを廃棄したり(VBR.2と呼ばれる)、セルのCLPを”1”としたりする(VBR.3と呼ばれる)と記載されている。この帯域監視機能をネットワークの入口のノードが所持することにより、ATMネットワークにおけるQoSを実現する。

【０００６】

【発明の解決しようとする課題】

従来技術1では転送動作の判定ルールに従いDSCPを判定した場合、ユーザが契約帯域を十分利用できない場合がある。判定ルールが音声、音声以外のパケットがそれぞれ優先パケットおよび非優先パケットであり、優先パケットの帯域が契約されている場合について説明する。従来技術１の帯域監視機能を所持する帯域監視装置は監視帯域以内の音声パケットを優先パケットと、監視帯域以上の音声

パケットおよび音声以外のパケットを非優先パケットと判定する。ユーザ送出のトラヒックが図8(a)の時、帯域監視機能通過後のトラヒックは図8(b)となる。図8(b)に示した斜線部分の音声パケット以外のパケットは、優先パケットが帯域監視以内であるにも関わらず、非優先パケットとして送信される。即ち、ユーザは優先パケットの契約帯域を十分利用できない。

【０００７】

一方、従来技術2でも同様の問題が発生する。従来技術2の帯域監視機能を所持する帯域監視装置は監視帯域以内のCLP=0のセルのみをCLP=0として送信する。ユーザ送出のトラヒックが図15(a)の時、帯域監視機能通過後のトラヒックは図15(b)となる。図15(b)に示した斜線部分のセルは、CLP=0のセルが帯域監視以内であるにも関わらず、CLP=1のセルとして送信される。即ち、ユーザはCLP=0の契約帯域を十分利用できない。

【０００８】

以上に述べた様に従来の技術ではネットワーク運用者が「契約帯域を有効に利用できるサービス」を提供することが出来なかった。そこで、本発明の第一の目的は、「契約帯域を有効に利用できるサービス」を提供することである。

【０００９】

また、従来の技術では「契約帯域を有効に利用できるサービス」を提供出来る帯域監視装置を提供することも出来なかった。本発明の第二の目的は、ネットワーク運用者が「契約帯域を有効に利用できるサービス」を提供出来る帯域監視装置を提供することである。

【００１０】

【課題を解決するための手段】

上記第一の目的は次の方法により解決される。パケットヘッダ内の優先度フィールドが「優先」の優先パケットを前記優先パケット以外のパケットよりも優先的に転送するネットワークにおいて、前記ネットワークを運用するのネットワーク運用者が前記ネットワークを利用するネットワーク利用者と優先パケットの帯域を契約している前記ネットワークに流入するパケットの帯域を監視する。前記ネットワーク利用者が前記優先度フィールドを設定してパケットをネットワーク

に送信している時に、優先パケット以外のパケットの優先度フィールドを優先パケットの優先度フィールドに対応する値に再設定する。

【００１１】

より具体的には、優先パケットが前記契約帯域未満の時に、優先パケット以外のパケットの優先度フィールドを優先パケットの優先フィールドに対応する値に再設定する。

【００１２】

また、前記ネットワーク利用者が優先度フィールドを設定せずネットワークにパケットを送信し、前記ネットワーク運用者と前記ネットワーク利用者間で契約された優先パケットの判定ポリシーに従い優先パケットと判定している時には、優先パケットと判定されないパケットの優先度フィールドを優先パケットの優先フィールドに対応する値に設定する。

【００１３】

また、前記ネットワーク利用者が優先度フィールドを設定せずネットワークにパケットを送信し、前記ネットワーク運用者と前記ネットワーク利用者間で契約された優先パケットの判定ポリシーに従い優先パケットと判定されたパケットの帯域が前記契約帯域未満の時に、優先パケットと判定されないパケットの優先度フィールドを優先パケットの優先フィールドに対応する値に設定する。

【００１４】

また、、前記帯域監視方式のアルゴリズムとしてバケツの深さを複数有するリーキーバケットアルゴリズムを使用し、前記バケツの深さを入力パケットに応じて切り替えて使用する。

【００１５】

上記第二の目的を達成するために、本発明の帯域監視装置では、入力パケットのアドレス情報、用途を識別する情報又は前記ネットワーク内の優先度を識別する情報であるネットワーク優先度のうち少なくとも一つの情報からパケットの一連のフロー(流れ)を検出して、前記フローの識別子であるフロー識別子と優先度であるフロー優先度を判定するフロー検出手段と、帯域監視のための制御情報である帯域監視制御情報と複数の前記ネットワーク優先度から構成されるエントリ

を一つあるいは複数所持する帯域監視テーブルと、前記フロー識別子に対応するエントリを帯域監視テーブルから読み出す帯域監視テーブル制御手段と、前記フロー優先度と前記帯域監視テーブル制御手段が読み出したエントリ内の帯域監視制御情報と現時刻を表すタイマーの値に基づいて前記入力パケットの遵守・違反の判定を行う監視結果判定手段と、前記監視結果判定手段の判定結果と前記帯域監視テーブル制御手段が読み出した複数のネットワーク優先度から前記入力パケットのネットワーク優先度を判定する優先度判定手段することを特徴とする。

【００１６】

また、他の帯域監視装置では、入力パケットのコネクション情報から前記コネクションの優先度であるコネクション優先度を判定するコネクション優先度判定手段と、帯域監視のための制御情報である帯域監視制御情報と複数の前記ネットワーク内の優先度を識別する情報であるネットワーク優先度から構成されるエントリを一つあるいは複数所持する帯域監視テーブルと、前記コネクション識別子に対応するエントリを帯域監視テーブルから読み出す帯域監視テーブル制御手段と、前記コネクション優先度と前記帯域監視テーブル制御手段が読み出したエントリ内の帯域監視制御情報と現時刻を表すタイマーの値に基づいて前記入力パケットの遵守・違反の判定を行う監視結果判定手段と、前記監視結果判定手段の判定結果と前記帯域監視テーブル制御手段が読み出した複数のネットワーク優先度から前記入力パケットのネットワーク優先度を判定する優先度判定手段することを特徴とする。

【００１７】

また、他の帯域監視装置においては、監視結果判定手段の前記帯域監視のアルゴリズムとしてバケツの深さを複数有するリーキーバケットアルゴリズムを使用し、前記帯域監視制御情報として優先パケット用のバケツの深さと優先パケット以外のパケット用のバケツの深さを所持することを特徴とする。

【００１８】

その他本願が解決しようとする課題、その解決手段は、「発明の実施の形態」の欄及び図面で明らかにされる。

【００１９】

【発明の実施の形態】

まず、帯域監視機能を所持する本発明のルータの概要を図1、図3および図4を用いて説明する。

【００２０】

図1は本発明のルータ100を示す。ルータ100はパケットが入力される入力回線101とパケットの受信処理を行うパケット受信回路160と、M個の受信側バッファ130-i(i=1～M)と、パケットを前記受信側バッファ130-iに振り分けて送信する受信側バッファ振り分け回路150と、ネットワーク内の優先度であるDSCPとパケットを出力する回線の識別子である出力回線番号を判定するヘッダ処理部140と、受信側バッファ130-iからパケットを読み出す受信側パケット送信回路120と、パケットを前記出力回線番号に基づきスイッチングするパケット中継処理手段110と、M個の送信側バッファ131-i(i=1～M)と、パケットを前記送信側バッファ131-iに振り分けて送信する送信側バッファ振り分け回路151と、送信側バッファ131-iからパケットを読み出す送信側パケット送信回路121と、パケットの送信処理を行うパケット送信回路161と、パケットが出力される出力回線102から構成される。図1には入力回線101と出力回線102がそれぞれ１回線づつ記載されているが、実際にはルータ100は、複数の入力回線101と出力回線102を有している。

【００２１】

図3はネットワークにおけるパケットのフォーマットの一例を示す。ネットワークにおけるパケットはヘッダ部310とデータ部320から構成される。ヘッダ部310は送信元アドレス（送信端末のアドレス）である送信元IPアドレス（Source IP Address：以下「SIP」という。）311と、宛先アドレス（受信端末のアドレス）である宛先IPアドレス（Destination IP Address：以下「DIP」という。）312と、プロトコル（＝上位アプリケーション）を表す送信元ポート（Source Port：以下「SPORT」という。）313と宛先ポート（Destination Port：以下「DPORT」という。）314とネットワーク内の優先度を表すDSCP315から構成される。また、データ部320はユーザのデータであるユーザデータ321から構成される。ヘッダ部310には前記情報以外にIPプロトコルの上位プロトコル等の情報も格納されてい

るが、前記情報と同様に後述の処理を実行することができる。図3のフォーマットは、トランスポート層のプロトコルがTCP（Transmission Control Protocol）またはUDP（User Datagram Protocol）で、ネットワーク層のプロトコルがIP（Internet Protocol）の場合を示したが、それ以外（例えばネットワーク層のプロトコルがIPX等）でも良い。

【００２２】

図4は本発明のルータ100内部におけるパケットのフォーマットの一例を示す。ルータ100内部におけるパケットのフォーマットはネットワークにおけるパケットのフォーマットに内部ヘッダ部330が備わる。この内部ヘッダ部330はパケットのバイト長を表すパケット長331とパケットが入力された回線の識別子である入力回線番号332と、パケットを出力される回線の識別子である出力回線番号333から構成される。

【００２３】

パケットが入力回線101より入力されるとパケット受信回路160は内部ヘッダ330を付加し、前記パケットのバイト長をカウントしてパケット長331に、パケットが入力した入力回線101の識別子を入力回線番号332に書き込む。さらに、前記パケットを蓄積すると同時に、内部ヘッダ部330とヘッダ部310から構成されるパケットヘッダ情報11をヘッダ処理部140に送信する。なお、出力回線番号333は無意味な値となっている。

【００２４】

ヘッダ処理部140の帯域監視部141は前記パケットヘッダ情報11からDSCPを判定し、前記DSCPから構成されるパケットDSCP情報12をパケット受信回路160に送信する。ヘッダ処理部140のルーティング処理部142は前記パケットヘッダ情報11内のDIP312よりパケットを出力する出力回線102を判定し、パケット出力回線情報13としてパケット受信回路160に送信する。

【００２５】

パケット受信回路160はパケットDSCP情報12とパケット出力回線情報13を受信すると前記情報をそれぞれDSCP315と出力回線番号333に書き込み、パケットを受信側バッファ振り分け回路150に送信する。受信側バッファ振り分け回路150はDS

CP315の値により送信する受信側バッファ130-iを判定し、前記受信側バッファ130-iへパケットを送信する。

【００２６】

受信側バッファ130-iは廃棄閾値132-iを所持し、DSCP315の値に基づいてバッファ蓄積制御を実行する。バッファ蓄積制御では受信側バッファ130-iはDSCPが優先パケットを表す場合、受信側バッファ130-iに空きが有るとパケットを蓄積し、空きが無いとパケットを廃棄する。非優先パケットを表す場合、前記廃棄閾値132-i以下のパケットが蓄積されているとパケットを蓄積し、前記廃棄閾値132-iを越えてパケットが蓄積されていると受信側バッファ130-iに空きが有ってもパケットを廃棄する。

【００２７】

受信側パケット送信回路120は受信側バッファ130-iに蓄積されているパケットの読み出し制御を実行する。読み出し制御として「完全優先制御」や「重みづけ巡回制御」等が知られている。「完全優先制御」では優先度の高い受信側バッファ130-iにパケットが蓄積されている場合、受信側バッファ130-iから蓄積された順番でパケットが読みだされる。優先度の高い受信側バッファ130-iにパケットが蓄積されていない時には、優先度の低い受信側バッファ130-iから蓄積された順番でパケットが読み出される。一方、「重みづけ巡回制御」では予め設定された比率に基づき受信側バッファ130-iからパケットが読み出される。

【００２８】

以上説明したバッファ蓄積制御と読み出し制御を組み合わせることにより、ルータ100内の優先パケットのQoSを実現する。

【００２９】

パケット中継処理手段110は出力回線番号333に従いパケットをスイッチングし、送信側バッファ振り分け回路151は前記DSCP315の値に基づき、パケットを送信側バッファ131-iに送信する。送信側バッファ131-iは受信側バッファ130-iと同様のパケット蓄積制御を、送信側パケット送信回路121は受信側パケット送信回路120と同様のパケット読み出し制御を行い優先パケットのQoSを確保する。パケット送信回路161は送信側バッファ131-iより読み出されたパケットを受信すると

、内部ヘッダ部330を削除し、出力回線102にパケットを送信する。

【００３０】

次に、図2および図5乃至図7を用いて、本発明の帯域監視部141の詳細動作について説明する。まず、図２を用いて本発明が想定するネットワーク構成について説明する。図2のネットワークは企業網A 210、企業網B 220、企業網C 230、企業網D240が公衆IPネットワークであるインターネット200によって接続されたネットワークである。インターネット200はエッジに位置するエッジルータA 202、エッジルータB 203と、コアに位置するバックボーンルータ201より構成される。また企業網A 210、企業網B 220、企業網C 230、企業網D240のインターネット200への出入り口にはそれぞれゲートウェイルータA211、ゲートウェイルータＢ221、ゲートウェイルータC231、ゲートウェイルータD241が配置されている。

【００３１】

本発明のルータ100は、インターネット200と企業網A210間で契約された優先パケットの帯域を監視するエッジルータA202として使用される。企業網A210のゲートウェイルータA211はパケットの優先・非優先を区別無く送信する場合(バウンダリマーキングケース)と、パケットの優先・非優先を区別して送信する場合(カスタマーマーキングケース)があるが、まずバウンダリマーキングケースについて説明する。なお、本実施例では帯域監視部141は音声パケットを優先的に優先パケットと判定する。

【００３２】

帯域監視のアルゴリズムとして固定長パケットであるセルの監視アルゴリズムであるcontinuousLeaky Bucket Algorithm(以下リーキーバケットアルゴリズム)を可変長パケットの帯域監視用に拡張したアルゴリズムを使用する。リーキーバケットアルゴリズムに関しては例えばThe ATM Forum Specification version 4.0の4.4.2章に記載されている。リーキーバケットアルゴリズムはある深さを持った穴の空いた漏れバケツのモデルで、バケツに水が入っている間は監視帯域で水は漏れ、セル到着時にはバケツに１セル分の固定量の水が注ぎ込まれる。セルの到着揺らぎを許容するためにバケツに深さを持ち、バケツが溢れない内は入力セルは遵守と、溢れると違反と判定する。本願ではパケット到着時に注ぎ込む水の

量を可変とすることにより、可変長パケットの帯域監視を実現する。

【００３３】

図5に帯域監視部141のブロック図を示す。帯域監視部141は帯域監視テーブル制御部560と、バケツ蓄積量判定部510と、監視結果判定部520と、DSCP判定部530と、フロー検出部540と、帯域監視テーブル550より構成される。

【００３４】

フロー検出部540はルータ固有の機能部である。ATM交換機は予めコネクションを設定し、入力セルのコネクション識別子により帯域監視制御情報を読み出し、その帯域監視制御情報を用いて帯域監視部が帯域監視を実行する（コネクション型通信）。一方、ルータ装置は予めコネクションを設定していないので、ルータ装置で帯域監視を行うためには、ルータ装置は入力パケット毎にヘッダ内の情報等により前記コネクション識別子の代わりのフロー識別子を判定するフロー検出手段が必要となる（コネクションレス型通信）。さらに、ルータは前記フロー識別子に対応する帯域監視制御情報を読み出し、その帯域監視制御情報を用いて帯域監視を実行する。なお、本願明細書では、ヘッダ内の情報等の情報を組み合わせて作成したパケット識別の条件をフロー条件と、フロー条件に一致する一連のトラヒックをフローと、フロー条件に入力パケットが一致するか否かを判定することをフロー検出と呼ぶ。

【００３５】

図6に帯域監視テーブル550のフォーマットを示す。前記帯域監視テーブル550はＮ個の帯域監視制御情報600-ｊ（ｊ=1～Ｎ）を所持する。帯域監視部141は一つの前記帯域監視制御情報600-ｊにより帯域を共有する一つないし複数のフローの帯域監視を実行する。本実施例では一つの帯域監視制御情報600-ｊにより、企業網A210が送出する音声パケットのフローと音声以外のパケットのフローを契約帯域で監視する。帯域監視制御情報600-ｊは後述のフロー優先度が「優先」のパケット用のバケツの深さTHR-A601-j(Byte)（Threshold-A)と、「非優先」のパケット用のバケツの深さTHR-B602-j（Byte)(Threshold-B)と、バケツが漏れる速度であり監視レートを表すPOLR603-j(Byte/sec)(Policing Rate)と、同一の帯域監視制御情報600-ｊ（ｊ=1～Ｎ）を参照するパケットが前回到着した時刻であるTS604-

j(sec)(Time Stamp)と、前パケットの帯域監視直後にバケツに蓄積されている水の量であるCNT605-j(Byte)(Count)と、帯域監視で「遵守」と判定され優先パケットとして転送されるパケットのDSCPであるDSCPC606-j(DSCP Conformance)と、「遵守」と判定され非優先パケットとして転送されるパケットのDSCPであるDSCPN607-j(DSCP non-Conformance)より構成される。なお、バケツの深さを表すTHR-A601-jとTHR-B602-jは、THR-A601-j≧THR-B602-jの関係がある。

【００３６】

図7に帯域監視部141のフローチャートを示す。帯域監視部141の処理は帯域監視開始処理700、バケツ蓄積量判定処理710、監視結果判定処理720、DSCP判定処理730である。後の3処理はそれぞれバケツ蓄積量判定部510と、監視結果判定部520と、DSCP判定部530が主に実行する。

【００３７】

帯域監視部141がパケットヘッダ情報11を受信すると、監視結果判定部520のパケット長蓄積手段522はパケット長331を、フロー検出部540はSIP311と、DIP312と、SPORT313と、DPORT314を蓄積する(ステップ701)。ステップ702では、フロー検出部540は蓄積された情報に基づいてフロー検出を行って入力パケットのフローの識別子であるフロー識別子およびフローの優先度であるフロー優先度を判定し、前記フロー識別子から構成されるフロー識別子情報14を帯域監視テーブル制御部560の帯域監視テーブル制御回路561へ、前記フロー優先度から構成されるフロー優先度情報17を監視結果判定部520のフロー優先度蓄積手段524へ送信する。本実施例では、音声パケットを優先的に優先パケットと判定する様に音声パケットのフロー優先度を「優先」に、音声パケット以外のフロー優先度を「非優先」とする。

【００３８】

帯域監視テーブル制御回路561は前記フロー識別子情報14を受信すると、フロー識別子情報14から帯域監視テーブル550のアドレスを作成し、帯域監視制御情報600-ｊを読み出し、THR-A601-jとTHR-B602-jを監視結果判定部520のTHR蓄積手段523に、POLR603-jとTS604-jとCNT605-jをバケツ蓄積量判定部510のそれぞれPOLR蓄積手段513、TS蓄積手段514、CNT蓄積手段515に、DSCPC606-jとDSCPN607-j

をそれぞれDSCP判定部530のDSCPC蓄積手段532とDSCPN蓄積手段533に蓄積する(ステップ703)。

【００３９】

バケツ蓄積量判定処理710では、バケツ蓄積量判定部510はパケット入力直前のバケツの水の量(バケツ蓄積量)を判定する。まず、バケツ蓄積量判定回路511は現時刻をカウントするタイマー512の値とTS蓄積手段514内の前パケットの到着時刻であるTS604-j(sec)との差分を計算し、前パケット到着からの経過時間(sec)を計算する(ステップ711)。次に経過時間(sec)にPOLR蓄積手段513内のPOLR603-j(Byte/sec)を乗じて、前パケット到着から漏れた水の量(バケツ減少量)を計算する(ステップ712)。さらに、CNT蓄積手段515内の前パケットの帯域監視直後のバケツ蓄積量であるCNT605-jからバケツ減少量を減算してパケットが入力する直前のバケツ蓄積量を判定する(ステップ713)。前記バケツ蓄積量の正負を判定し(ステップ714)、判定結果が負の場合にはバケツ蓄積量を”０”(バケツは空)に修正する(ステップ715)。

【００４０】

監視結果判定処理720では、監視結果判定部520の監視結果判定回路521は入力パケットのパケット長に相当する水がバケツに入るか否かを判定する。まず、バケツ蓄積量判定処理710で判定されたバケツ蓄積量(Byte)にパケット長(Byte)を加算する(ステップ721)。次に、フロー検出部540が送信しているフロー優先度情報17をフロー優先度蓄積手段524に蓄積する。この蓄積情報に基づき検索処理は分岐する(ステップ722)。前記蓄積情報が「優先」の場合にはTHR蓄積手段523に蓄積されている優先パケット用のバケツの深さTHR-A601-jと前記加算値との大小比較を行う(ステップ723)。バケツ蓄積量＋パケット長＞THR-A601-jであって、パケット長に相当する水を入力した場合にバケツが溢れてしまう時には、入力パケットを違反パケットと判定して「違反」を表す帯域監視結果情報15をDSCP判定部530のDSCP判定回路531と帯域監視テーブル制御部560の帯域監視テーブル制御回路561に送信する(ステップ726)。一方、バケツ蓄積量＋パケット長≦THR-A601-jの時には、入力パケットを遵守パケットと判定し、「遵守」を表示した帯域監視結果情報15をDSCP判定回路531と帯域監視テーブル制御回路561に、「バケ

ツ蓄積量＋パケット長」の値をバケツ蓄積量情報16として帯域監視テーブル制御回路561に送信する(ステップ725)。ステップ722の参照結果が非優先の場合にはバケツ蓄積量＋パケット長の値がTHR蓄積手段523に蓄積されている非優先パケット用のバケツの深さTHR-B602-jと前記加算値との大小比較を行う(ステップ724)。バケツ蓄積量＋パケット長＞THR-B602-jの時には前記ステップ726を、バケツ蓄積量＋パケット長≦THR-B602-jの時には、前記ステップ725を実行する。

【００４１】

ステップ722およびステップ724は本発明固有の処理である。企業網A210が音声パケットを契約帯域以未満で送信している場合には、音声パケットだけではバケツに水が蓄積されず音声パケット以外のパケットも「遵守」と判定される。一方、ユーザが音声パケットを契約帯域以上で送信している場合には、常にTHR-B602-jを越えてバケツに水が蓄積されるため、音声パケットのみ「遵守」と判定される。

【００４２】

帯域監視テーブル制御回路561は「遵守」を表示した帯域監視結果情報15を受信すると、バケツ蓄積量情報16とタイマー512の値を、それぞれ帯域監視直後のバケツ蓄積量およびパケットの到着時刻として、パケットのCNT605-jとTS604-jに書き込む(ステップ727)。帯域監視テーブル制御回路561は「違反」を表示した帯域監視結果情報15を受信すると前記ステップ727を行わない。

【００４３】

DSCP判定処理730では、DSCP判定部530は帯域監視結果情報15に基づいてDSCPを判定する。DSCP判定回路531は帯域監視結果情報15が「遵守」の場合、DSCPC蓄積手段532内のDSCPを入力パケットのDSCPと判定し、前記DSCPより構成されるパケットDSCP情報12をパケット受信回路160に送信する(ステップ731)。「違反」の場合、DSCPN蓄積手段523内のDSCPを入力パケットのDSCPと判定し、前記DSCPより構成されるパケットDSCP情報12 をパケット受信回路160に送信する(ステップ732)。

【００４４】

従来技術１の帯域監視機能を所持する帯域監視装置は監視帯域以内の音声パケ

ットを優先パケットと、監視帯域以上の音声パケットおよび音声以外のパケットを非優先パケットと判定する。図8(a)に示すトラヒックが入力されると、帯域監視後のトラヒックは図8(b)の様になる。図8(b)に示した斜線部分の音声パケット以外のパケットは、優先パケットが帯域監視以内であるにも関わらず、非優先パケットとして送信される。即ち、企業網A210の管理者は優先パケットの契約帯域を十分利用できない。本発明の帯域監視部141は新たに閾値THR-B602-jを所持して音声パケットの帯域が契約帯域以下であってバケツ蓄積量がTHR-B602-j以下の時には、音声パケット以外のパケットを優先パケットと判定する。本発明の帯域監視部141による帯域監視後のトラヒックは図8(c)の様になり、企業網A210の管理者は契約帯域を有効活用できる。

【００４５】

以上の実施例ではゲートウェイルータA211が２種のフロー優先度が異なるパケット(音声パケットとそれ以外のパケット)を送信する場合について説明した。4種のフロー優先度が異なるパケットを送信する場合について説明する。以下ではゲートウェイルータA211は音声、トランザクションデータ、E-mail、その他のパケットの4種のフロー優先度が異なるパケットを送信する。なお、優先度は音声＞トランザクションデータ＞E-mail＞その他のパケットの順である。図9に帯域監視部941のブロック図を、図10に帯域監視テーブル950のフォーマットを、図11に監視結果判定処理1120のフローチャートを示す。以下、前記２種のパケットを送信する場合との差分を説明する。帯域監視テーブル950は帯域監視テーブル550に比べて、THR-C1008-j(j=１～N)とTHR-D1009-jを新たに備える。なお、THR-A601-j≧THR-B602-j≧THR-C1008-j≧THR-D1009-jの関係がある。フロー優先度が２種の場合のステップ702はフロー検出部940がフロー識別子とフロー優先度「優先度1～4」を判定し、フロー識別子からなるフロー識別子情報14を帯域監視テーブル制御部560の帯域監視制御テーブル制御回路561に、4つのフロー優先度からなるフロー優先度情報20をフロー優先度蓄積手段924に送出するステップ1102となる。さらに、ステップ703はTHR-A601-j、THR-B602-jに加えて THR-C1008-j、THR-D1009-jもTHR蓄積手段923に蓄積するステップ1103となる。

【００４６】

監視結果判定処理1120では、ステップ722～724がステップ1122～1126となる。ステップ1122ではフロー検出部940が送信しているフロー優先度情報20をフロー優先度蓄積手段924が蓄積し、この蓄積情報に基づき処理動作が４つに分岐する。前記蓄積情報が「優先度1」、「優先度２」、「優先度３」、「優先度４」の場合には、それぞれTHR-A601-j、THR-B602-j、THR-C1008-j、THR-D1009-jとステップ721において計算された「バケツ蓄積量＋パケット長」との大小比較を行い、遵守・違反の判定を行う(ステップ1123～1126)。

【００４７】

以上に述べた様にゲートウェイルータA211が4種のフロー優先度が異なるパケットを送信する場合には、４個のバケツの深さを所持することにより図12に示した様にフロー優先度の高いパケットから順番に契約帯域に詰め込むことが出来る。同様に、H(＞2)種のフロー優先度が異なるパケットを送信する場合には、H個のバケツの深さを所持することによりフロー優先度の高いパケットから順番に契約帯域に詰め込むことが出来る。

【００４８】

これまで、企業網A210が優先度を区別せずに送信するバウンダリマーキングケースにおける帯域監視部141や帯域監視部941の動作について説明した。企業網A210がパケットの優先度を区別して送信するカスタママーキングケースにおける帯域監視部141の動作について説明する。図2のインターネット200と企業網A210間で優先パケットの帯域が契約されており、ゲートウェイルータA211は図13(a)の様に優先パケット・非優先パケットをDSCPにより区別して送信する。エッジルータA202は帯域監視を行って前記DSCPの再割り当てを行う。本発明を適用した帯域監視部141を所持するルータ100が前記エッジルータA202として使用される。バウンダリマーキングケースではステップ701において帯域監視部141がパケットヘッダ情報11を受信すると、フロー検出部540はSIP311と、DIP312と、SPORT313と、DPORT314を蓄積していた。カスタマーマーキングケースでは前記情報に加えてヘッダ部310内のDSCP315も蓄積してフロー検出に使用する。これら以外の動作はバウンダリマーキングケースの帯域監視部141の動作と同一である。

【００４９】

従来技術2では優先パケットをゲートウェイルータA211が送信していない時にも、非優先パケットのDSCPは変更されず、企業網A210の管理者は契約帯域を有効に活用できない(図13(b))。一方、本発明の帯域監視部141を所持するルータ100を前記エッジルータA202として使用すると、優先パケットをゲートウェイルータA211が送信していない時には、DSCPの優先度を上げることにより企業網A210の管理者は契約帯域を有効に活用できる(図13(c))。

【００５０】

これまでの実施例では、コネクションレス型通信の帯域監視について説明してきた。ATMやフレームリレー等のコネクション型通信の帯域監視部1441のブロック図を図14に示す。フロー検出の必要が無いため、フロー検出部540は、コネクション優先度判定部1440となる。このコネクション優先度判定部1440はコネクション識別子情報18内のコネクション識別子からコネクションの優先度を判定し、コネクション優先度情報19としてコネクション優先度蓄積手段1424に送信する。帯域監視テーブル制御回路1461はフロー識別子の代わりにコネクション識別子から帯域監視テーブル550のアドレスを生成して帯域監視制御情報600-ｊを読み出す。また、監視結果判定回路1421はコネクション優先度蓄積手段1424内のコネクション優先度に基づいて、パケットの遵守・違反を判定する。以上の処理以外はコネクション型通信の帯域監視部141の動作と同一である。

【００５１】

また、ネットワークの優先度をIPヘッダのDSCPに限定して説明してきたがATMセルのヘッダ内のCLP(Cell Loss Priority)ビットやフレームリレーのフレームヘッダ内のDE(Delete Enable)ビットもDSCPと同様に処理することが出来る。ゲートウェイルータA211がATMのCLPにマーキングした場合(カスタマーマーキングケース)に送出するトラヒックを図15(a)に、従来技術2を用いて帯域監視した場合の帯域監視後のトラヒックを図15(b)に、本発明を適用したエッジルータA202を使用した場合の帯域監視後のトラヒックを図15(c)に示した。従来技術2ではCLP=0のセルをゲートウェイルータA211が送信していない時にも、CLP=1のセルのCLPは変更されず、企業網A210の管理者は契約帯域を有効に活用できない。一方、

本発明を適用した帯域監視部141を所持するルータ100をエッジルータA202として使用すると、CLP=0のセルをゲートウェイルータA211が送信していない時には、CLP=1のセルをCLP=０とネットワーク内の優先度が上がるため、企業網A210の管理者は契約帯域を有効に活用できる。

【００５２】

【発明の効果】

パケットヘッダ内の優先度フィールドが「優先」の優先パケットを優先パケット以外のパケットである非優先パケットよりも優先的に転送するネットワークであって、前記ネットワークのネットワーク運用者が前記ネットワークを利用するネットワーク利用者と優先パケットの帯域を契約し、前記ネットワークの入口のノードで優先パケットの帯域を監視しているネットワークにおいて、以下の効果がある。

【００５３】

前記ネットワーク利用者が優先度フィールドを設定してネットワークに送信し、優先パケットが前記契約帯域未満の時、前記ネットワークの入口のノードにおいて優先パケット以外のパケットの優先度フィールドを優先パケットに対応する値に再設定することにより、ネットワーク運用者が「契約帯域を有効に利用できるサービス」を提供できる。また、前記ネットワークの入口のノードに非優先パケットの優先度フィールドを優先パケットに対応する値に再設定する帯域監視部を備えることにより、「契約帯域を有効に利用できるサービス」を提供出来る帯域監視装置を提供できる。

【００５４】

前記ネットワーク利用者が優先度フィールドを設定せずネットワークに送信し、前記ネットワークの入口のノードが前記ネットワーク運用者と前記ネットワーク利用者間で契約された優先パケットの判定ポリシーに従って優先パケットと非優先パケットの判定を行っている時には、下記の効果がある。　前記判定において優先パケットと判定されたパケットの帯域が前記契約帯域未満の時には、非優先パケットと判定されたパケットの優先度フィールドを優先パケットに対応する値に設定することにより、「契約帯域を有効に利用できるサービス」を提供でき

る。また、前記ネットワークの入口のノードが前記判定の際に非優先パケットと判定したパケットの優先度フィールドを優先パケットに対応する値に再設定する帯域監視部を備えることにより、「契約帯域を有効に利用できるサービス」を提供出来る帯域監視装置を提供できる。

【図面の簡単な説明】

【図１】

本発明のルータの構成を示すブロック図。

【図２】

インターネットの構成図。

【図３】

ネットワークにおけるパケットのフォーマットを示す図。

【図４】

本発明のルータにおけるパケットのフォーマットを示す図。

【図５】

本発明の帯域監視部141の構成を示すブロック図。

【図６】

帯域監視テーブル550のフォーマットを示す図。

【図７】

本発明を適用した帯域監視部141のフローチャート。

【図８】

(a)　企業網A210が送信している音声パケットと音声パケット以外のトラヒックの時間変化を表す図。

(b)　従来技術１を適用した帯域監視装置通過後のトラヒックの時間変化を表す図。

(c)　本発明を適用した帯域監視装置141を所持するルータ通過後のトラヒックの時間変化を表す図。

【図９】

本発明を適用した帯域監視部941の構成を示すブロック図。

【図１０】

帯域監視テーブル950のフォーマットを示す図。

【図１１】

本発明を適用した監視結果判定部920のフローチャート。

【図１２】

本発明を適用した帯域監視装置141を所持するルータ通過後のトラヒックの時間変化を表す図(企業網A210送出トラヒックが４種の場合)。

【図１３】

(a)　企業網A210が送信している優先パケットと非優先パケットのトラヒックの時間変化を表す図。

(b)　従来技術２を適用した帯域監視装置通過後のトラヒックの時間変化を表す図。

(c)　本発明を適用した帯域監視部941を所持するルータ通過後のトラヒックの時間変化を表す図。

【図１４】

本発明を適用したの帯域監視部1441の構成を示すブロック図。

【図１５】

(a)　企業網A210が送信しているCLP=0とCLP=1のトラヒックの時間変化を表す図。　(b)　従来技術２を適用した帯域監視装置通過後のトラヒックの時間変化を表す図。

(c)　本発明を適用した帯域監視装置通過後のトラヒックの時間変化を表す図。

【符号の説明】

11…パケットヘッダ情報

12…パケットDSCP情報

13…パケット出力回線情報

14…フロー識別子情報

15…帯域監視結果情報

16…バケツ蓄積量情報

17…フロー優先度情報

18…コネクション識別子情報

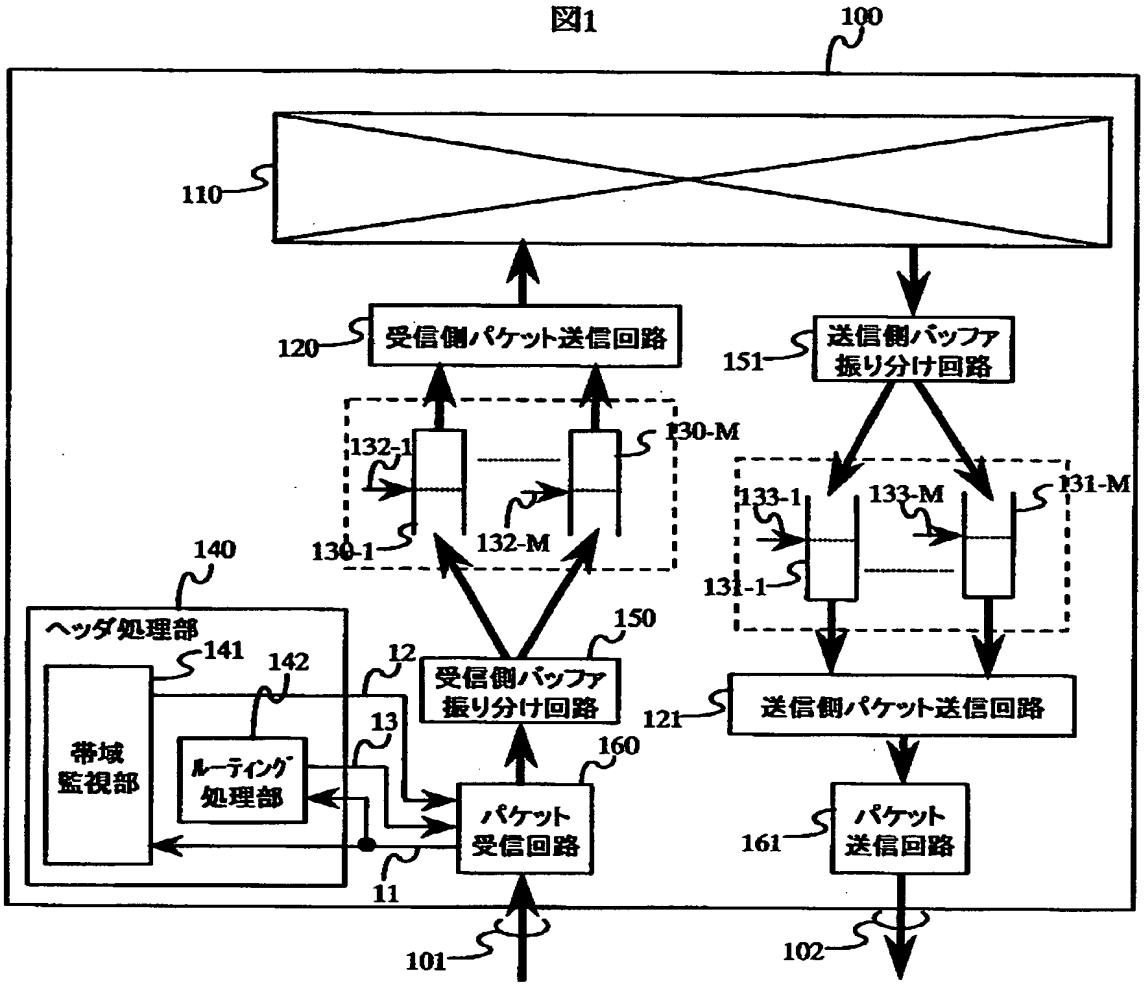
19…コネクション優先度情報

20…フロー優先度情報。

【書類名】　図面

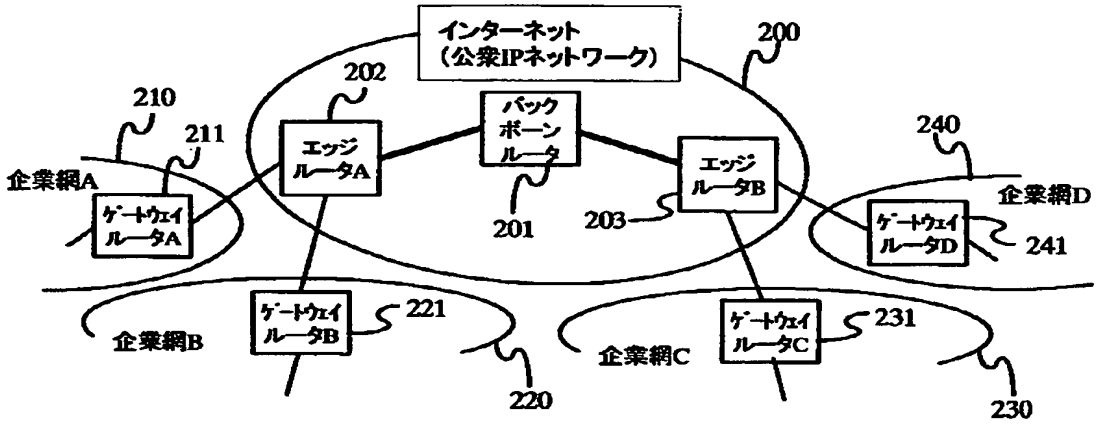
【図１】

図1


100
110
120
受信側パケット送信回路
151
送信側バッファ振り分け回路
130-M
132-1
130-1
132-M
133-1
133-M
131-M
131-1
140
ヘッダ処理部
141
142
12
150
受信側バッファ振り分け回路
121
送信側パケット送信回路
13
160
帯域監視部
ルーティング処理部
パケット受信回路
161
パケット送信回路
11
101
102

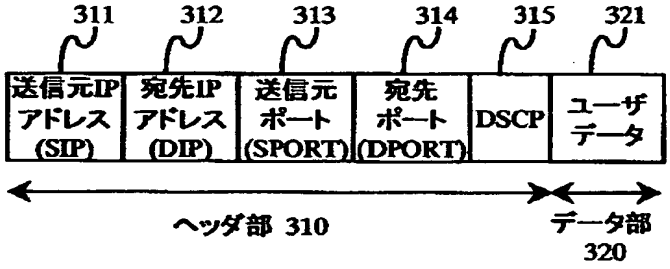
【図２】

図2



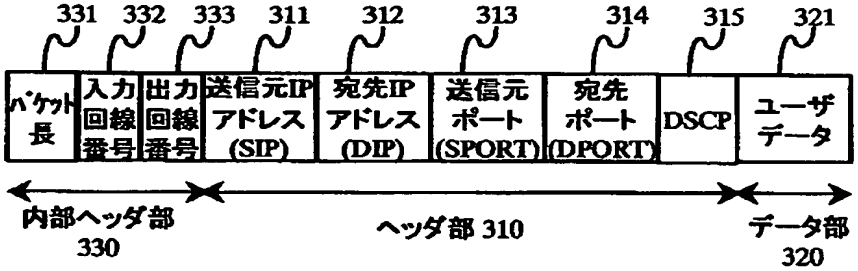
【図３】

図3



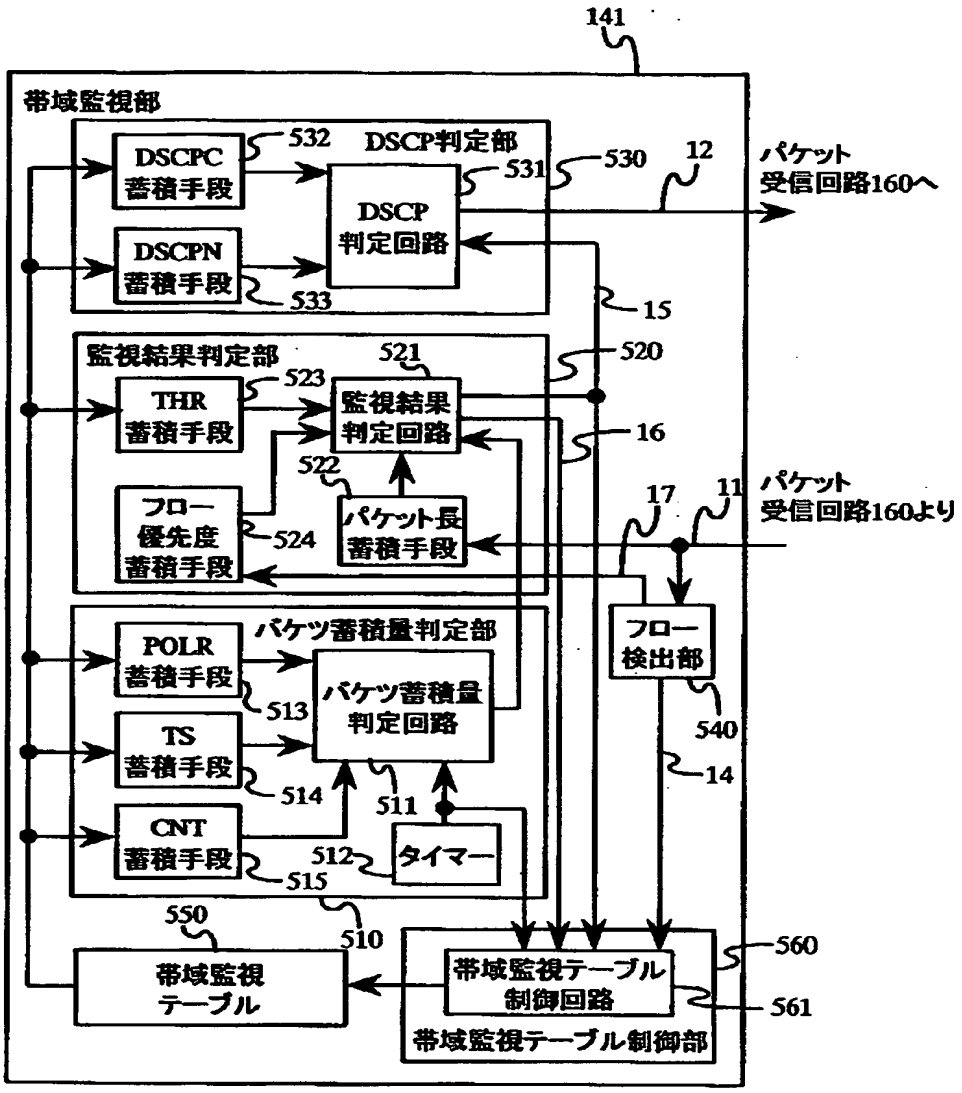
【図４】

図4



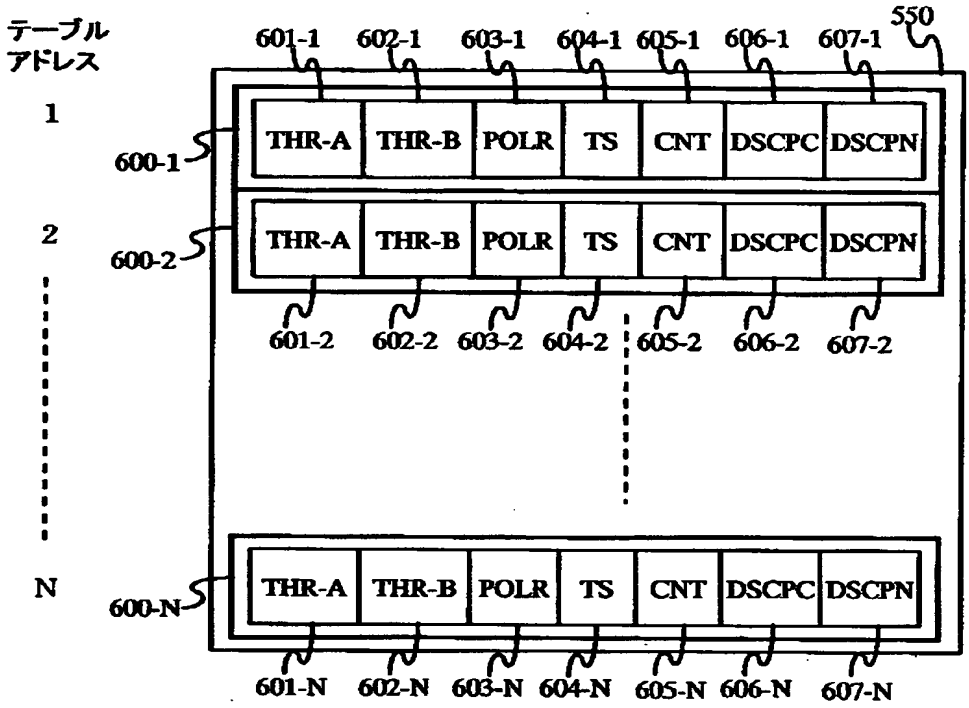
【図５】

図5


141
帯域監視部
DSCPC
蓄積手段
532
DSCP判定部
DSCP
判定回路
531
530
12
パケット
受信回路160へ
DSCPN
蓄積手段
533
15
監視結果判定部
521
520
THR
蓄積手段
523
監視結果
判定回路
16
522
フロー
優先度
蓄積手段
524
パケット長
蓄積手段
17
11
パケット
受信回路160より
フロー
検出部
540
14
パケツ蓄積量判定部
POLR
蓄積手段
513
パケツ蓄積量
判定回路
TS
蓄積手段
514
511
CNT
蓄積手段
512
タイマー
515
550
510
帯域監視
テーブル
帯域監視テーブル
制御回路
560
561
帯域監視テーブル制御部

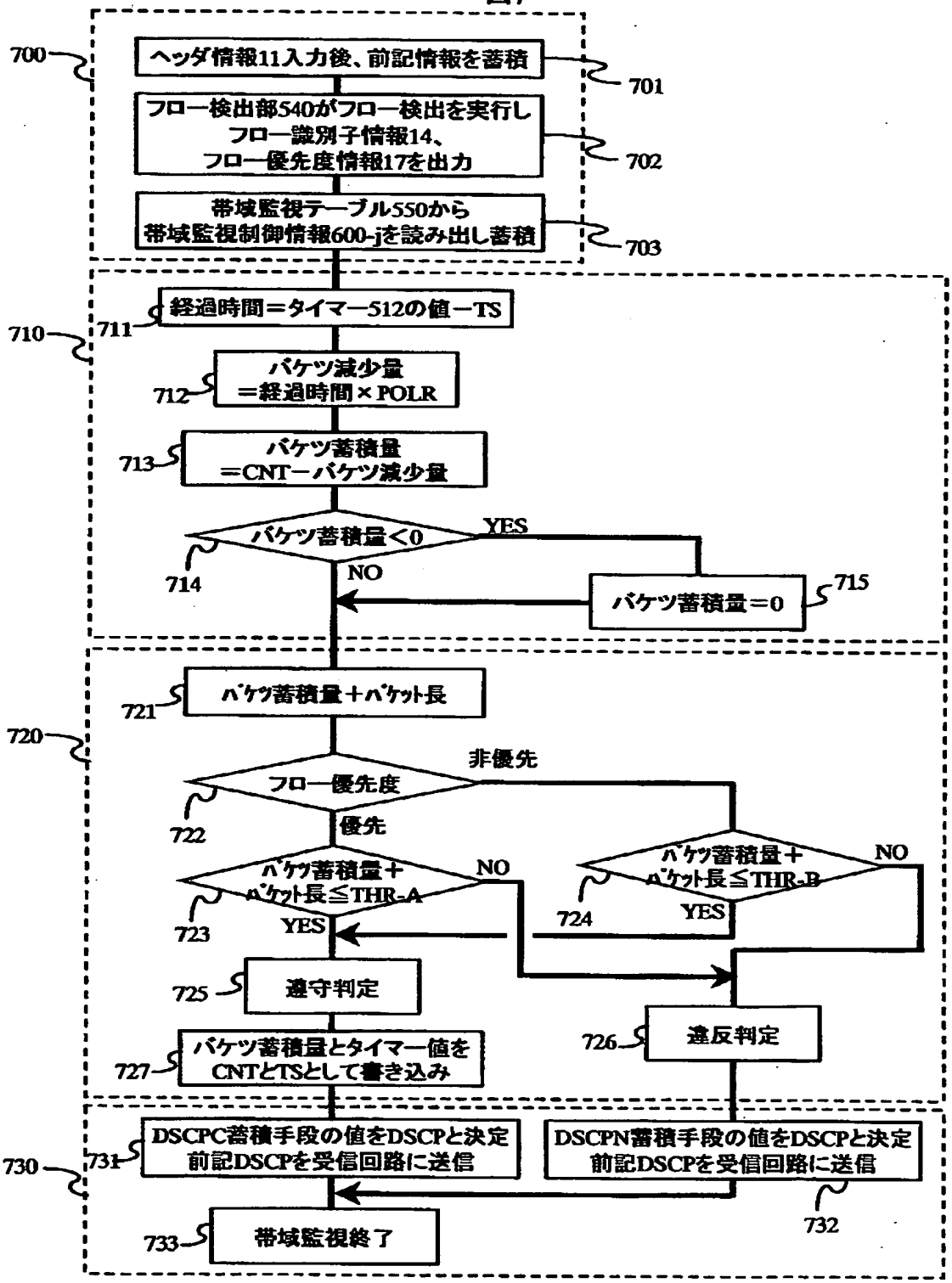
【図６】

図6


テーブル
アドレス
1
2
N
550
601-1
602-1
603-1
604-1
605-1
606-1
607-1
600-1
600-2
600-N
THR-A
THR-B
POLR
TS
CNT
DSCPC
DSCPN
601-2
602-2
603-2
604-2
605-2
606-2
607-2
601-N
602-N
603-N
604-N
605-N
606-N
607-N

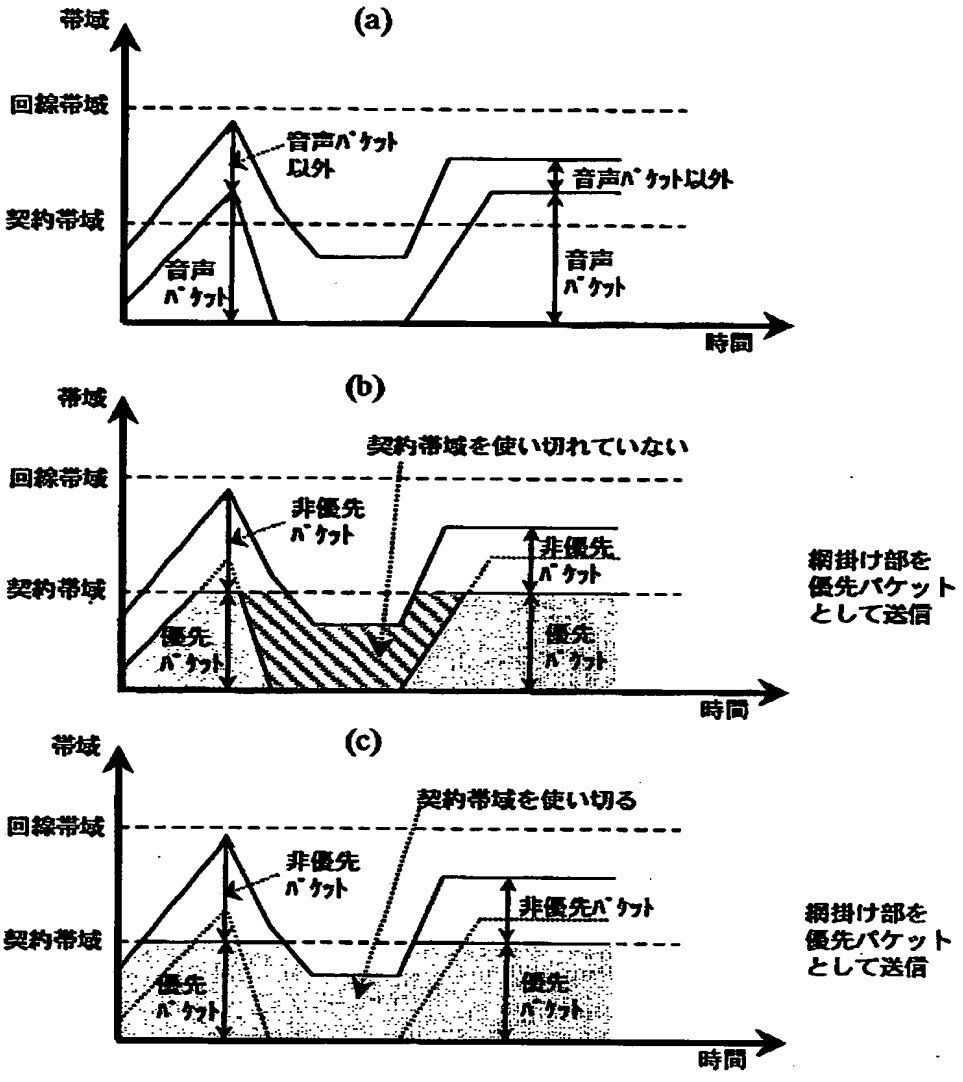
【図７】

図7


700
ヘッダ情報11入力後、前記情報を蓄積
701
フロー検出部540がフロー検出を実行し
フロー識別子情報14、
フロー優先度情報17を出力
702
帯域監視テーブル550から
帯域監視制御情報600-jを読み出し蓄積
703
710
711
経過時間＝タイマー512の値－TS
712
バケツ減少量
＝経過時間×POLR
713
バケツ蓄積量
＝CNT－バケツ減少量
714
バケツ蓄積量<0
YES
NO
715
バケツ蓄積量＝0
720
721
ﾊﾞｹﾂ蓄積量＋ﾊﾟｹｯﾄ長
非優先
フロー優先度
722
優先
723
ﾊﾞｹﾂ蓄積量＋
ﾊﾟｹｯﾄ長≦THR-A
NO
YES
724
ﾊﾞｹﾂ蓄積量＋
ﾊﾟｹｯﾄ長≦THR-B
NO
YES
725
遵守判定
726
違反判定
727
バケツ蓄積量とタイマー値を
CNTとTSとして書き込み
730
731
DSCPC蓄積手段の値をDSCPと決定
前記DSCPを受信回路に送信
DSCPN蓄積手段の値をDSCPと決定
前記DSCPを受信回路に送信
732
733
帯域監視終了

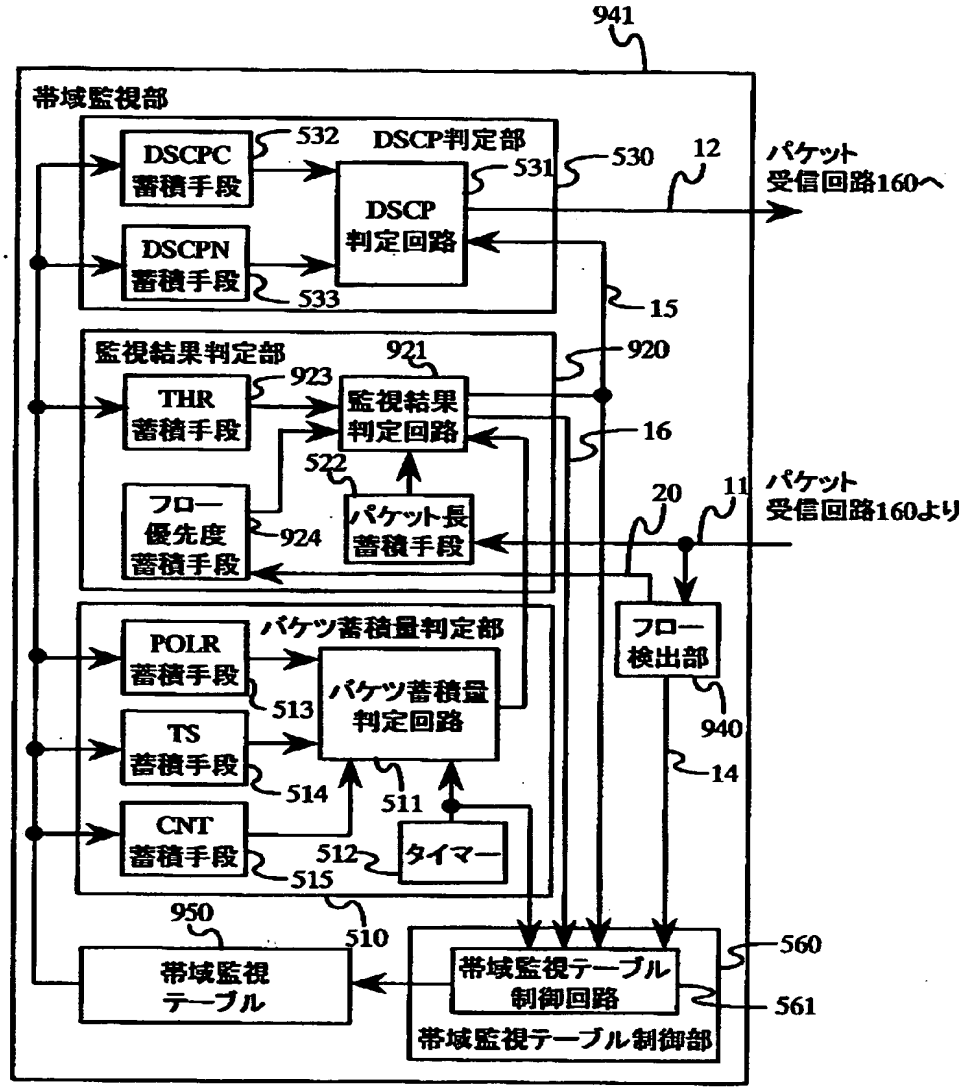
【図８】

図8


(a)
帯域
回線帯域
契約帯域
音声パケット以外
音声パケット
音声パケット以外
音声パケット
時間
(b)
帯域
契約帯域を使い切れていない
回線帯域
契約帯域
非優先パケット
優先パケット
非優先パケット
優先パケット
時間
網掛け部を優先パケットとして送信
(c)
帯域
契約帯域を使い切る
回線帯域
契約帯域
非優先パケット
優先パケット
非優先パケット
優先パケット
時間
網掛け部を優先パケットとして送信

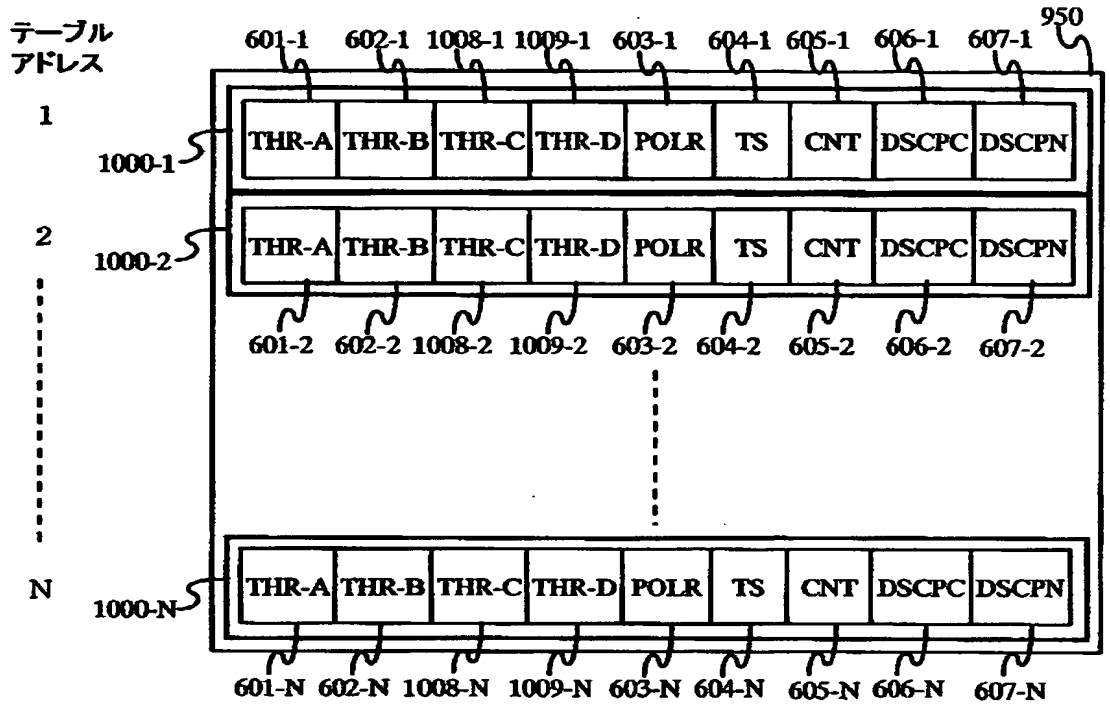
【図９】

図9


941
帯域監視部
DSCPC
蓄積手段
532
DSCP判定部
DSCP
判定回路
531
530
12
パケット
受信回路160へ
DSCPN
蓄積手段
533
15
監視結果判定部
921
920
THR
蓄積手段
923
監視結果
判定回路
16
522
フロー
優先度
蓄積手段
924
パケット長
蓄積手段
20
11
パケット
受信回路160より
フロー
検出部
940
14
パケツ蓄積量判定部
POLR
蓄積手段
513
パケツ蓄積量
判定回路
TS
蓄積手段
514
511
CNT
蓄積手段
512
タイマー
515
950
510
帯域監視
テーブル
帯域監視テーブル
制御回路
560
561
帯域監視テーブル制御部

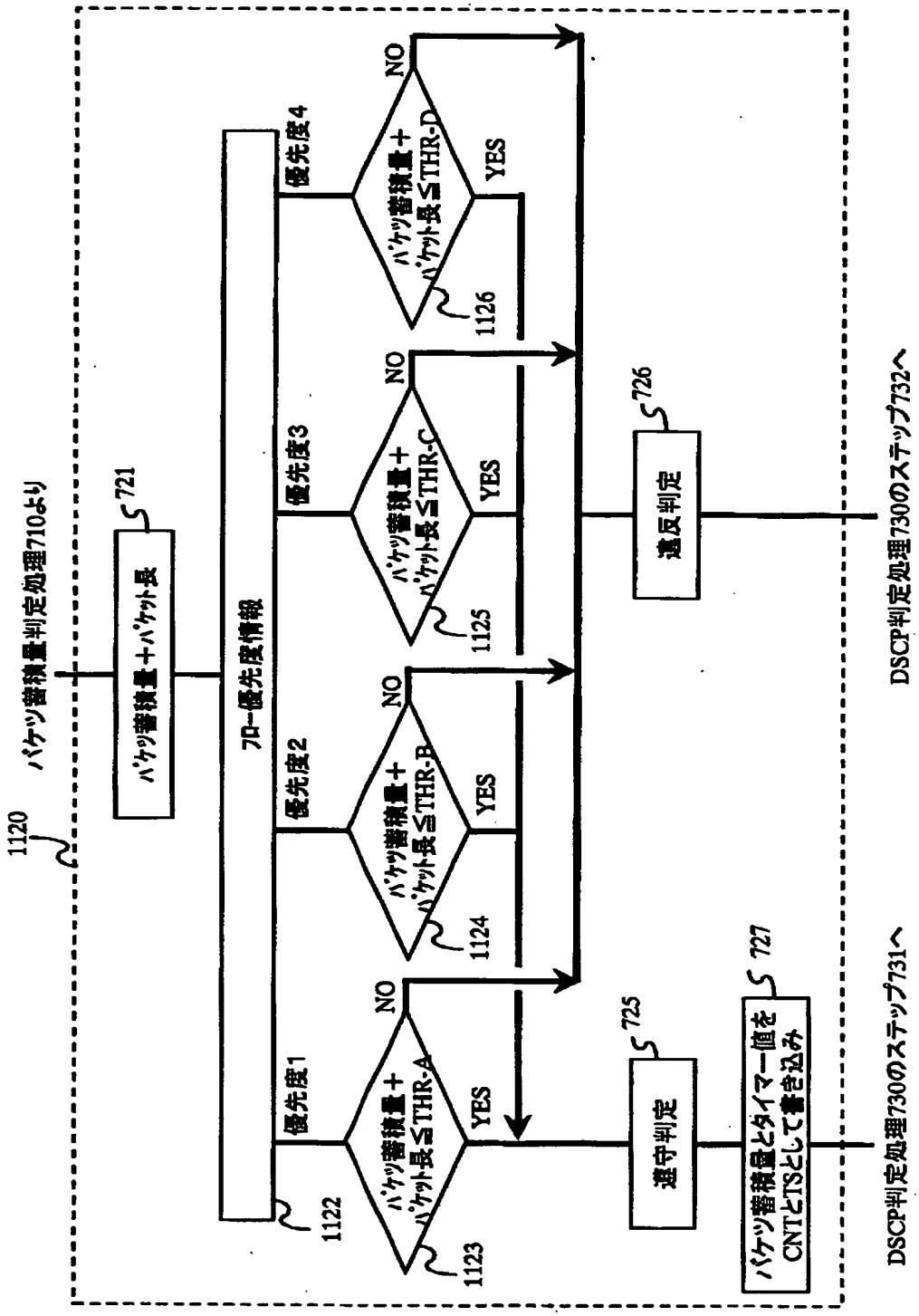
【図１０】

図10


テーブル
アドレス
1
2
N
1000-1
1000-2
1000-N
950
601-1
602-1
1008-1
1009-1
603-1
604-1
605-1
606-1
607-1
THR-A
THR-B
THR-C
THR-D
POLR
TS
CNT
DSCPC
DSCPN
601-2
602-2
1008-2
1009-2
603-2
604-2
605-2
606-2
607-2
601-N
602-N
1008-N
1009-N
603-N
604-N
605-N
606-N
607-N

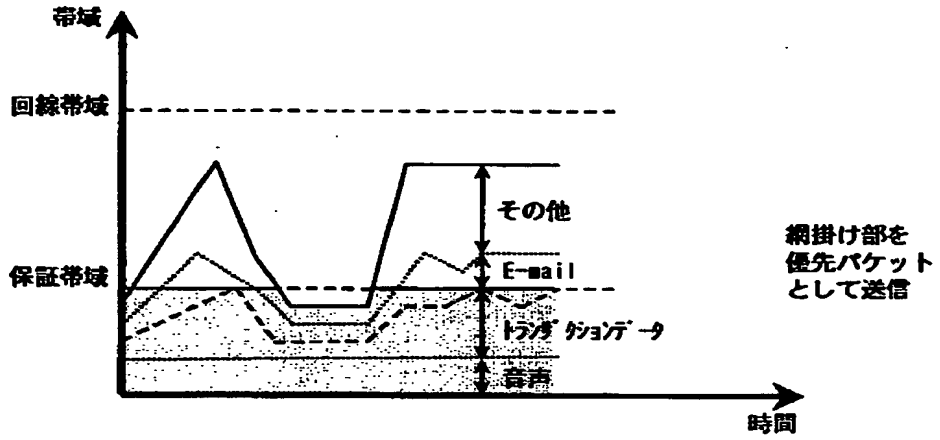
【図１１】

図11


パケット蓄積量判定処理710より
1120
パケット蓄積量＋パケット長
721
フロー優先度情報
優先度4
優先度3
優先度2
優先度1
1122
パケット蓄積量＋パケット長≦THR-D
1126
パケット蓄積量＋パケット長≦THR-C
1125
パケット蓄積量＋パケット長≦THR-B
1124
パケット蓄積量＋パケット長≦THR-A
1123
NO
YES
726
違反判定
725
遵守判定
727
パケット蓄積量とタイマー値をCNTとTSとして書き込み
DSCP判定処理730のステップ732へ
DSCP判定処理730のステップ731へ

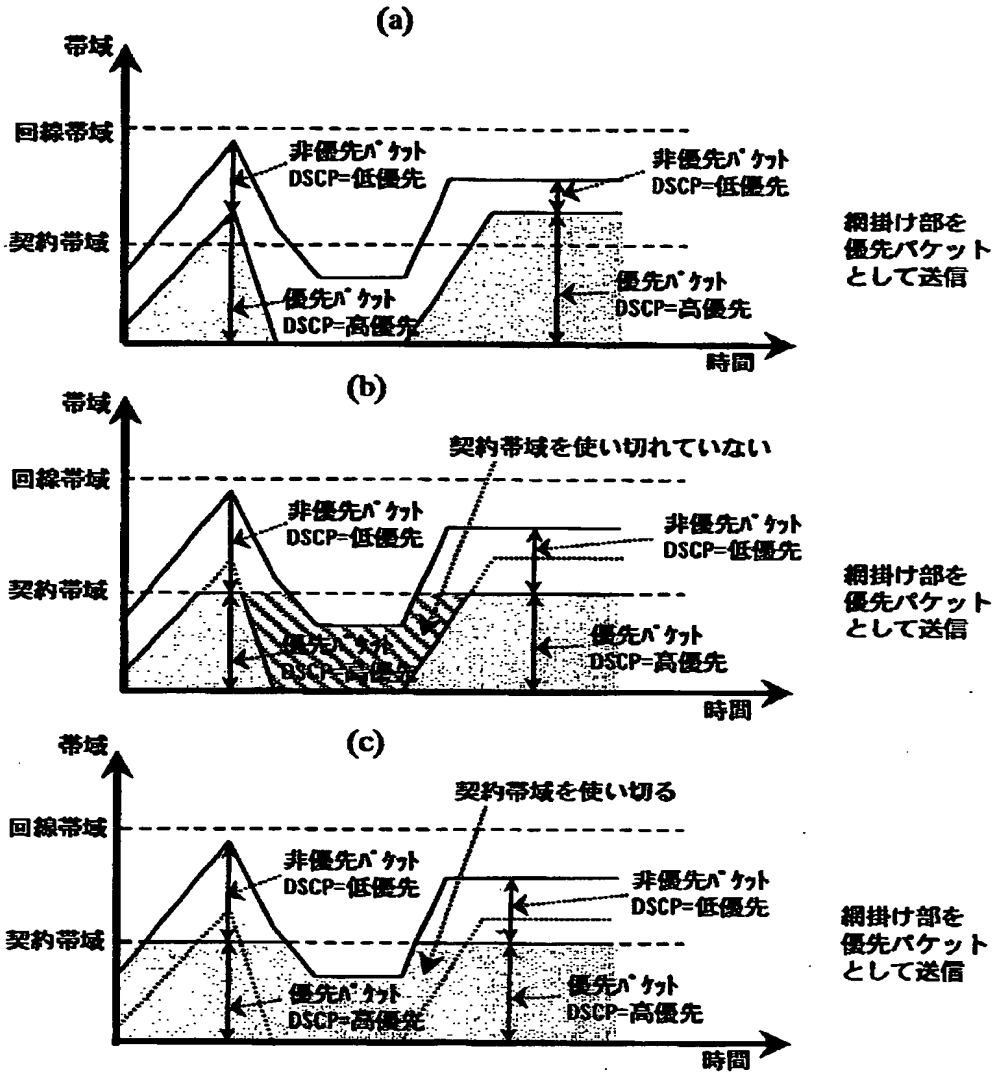
【図１２】

図12


帯域
回線帯域
保証帯域
その他
E-mail
ﾄﾗﾝｻﾞｸｼｮﾝﾃﾞｰﾀ
音声
時間
網掛け部を
優先パケット
として送信

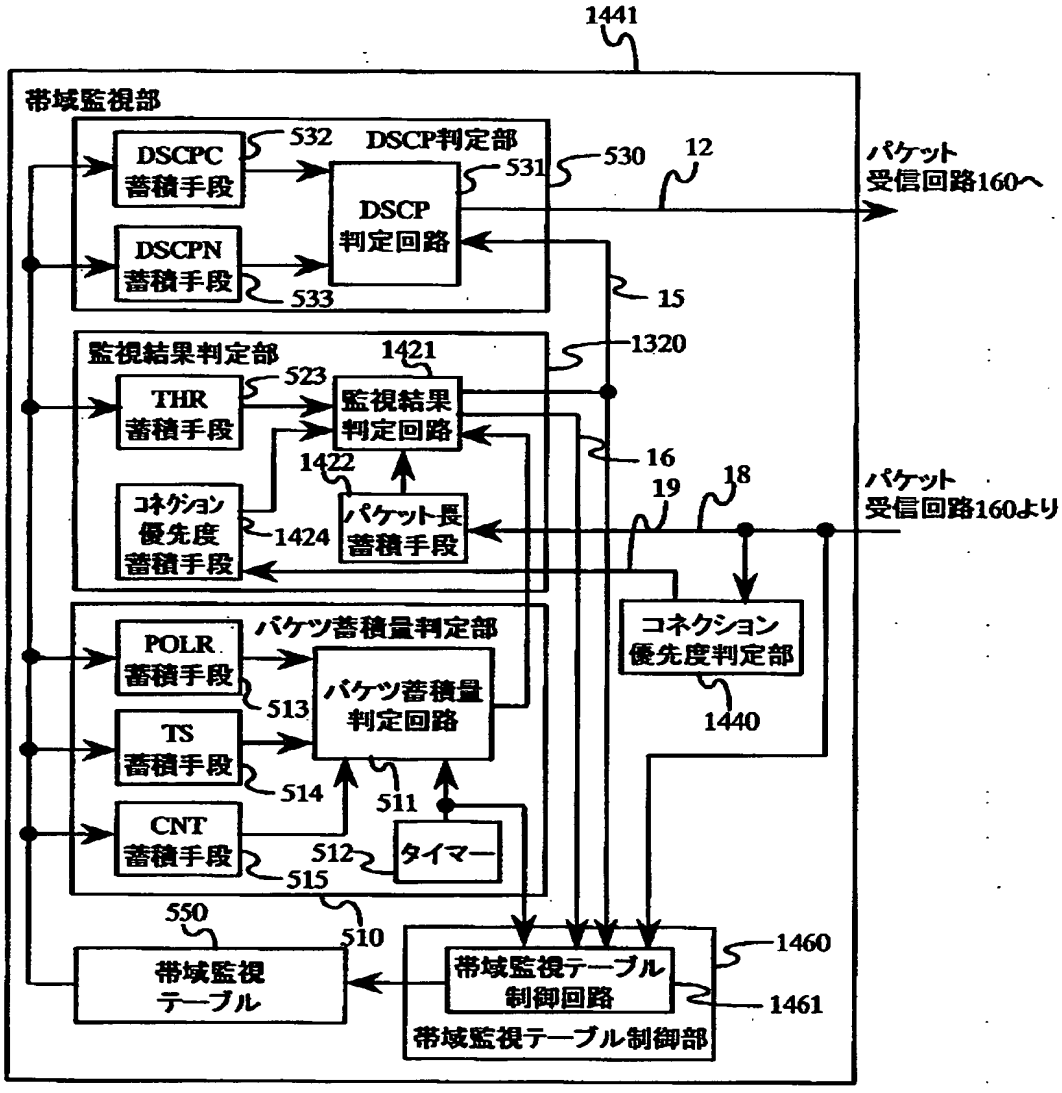
【図１３】

図13


(a)
帯域
回線帯域
契約帯域
非優先ﾊﾟｹｯﾄ
DSCP=低優先
非優先ﾊﾟｹｯﾄ
DSCP=低優先
優先ﾊﾟｹｯﾄ
DSCP=高優先
優先ﾊﾟｹｯﾄ
DSCP=高優先
時間
網掛け部を
優先パケット
として送信
(b)
帯域
契約帯域を使い切れていない
回線帯域
非優先ﾊﾟｹｯﾄ
DSCP=低優先
非優先ﾊﾟｹｯﾄ
DSCP=低優先
契約帯域
優先ﾊﾟｹｯﾄ
DSCP=高優先
時間
網掛け部を
優先パケット
として送信
(c)
帯域
契約帯域を使い切る
回線帯域
非優先ﾊﾟｹｯﾄ
DSCP=低優先
非優先ﾊﾟｹｯﾄ
DSCP=低優先
契約帯域
優先ﾊﾟｹｯﾄ
DSCP=高優先
優先ﾊﾟｹｯﾄ
DSCP=高優先
時間
網掛け部を
優先パケット
として送信

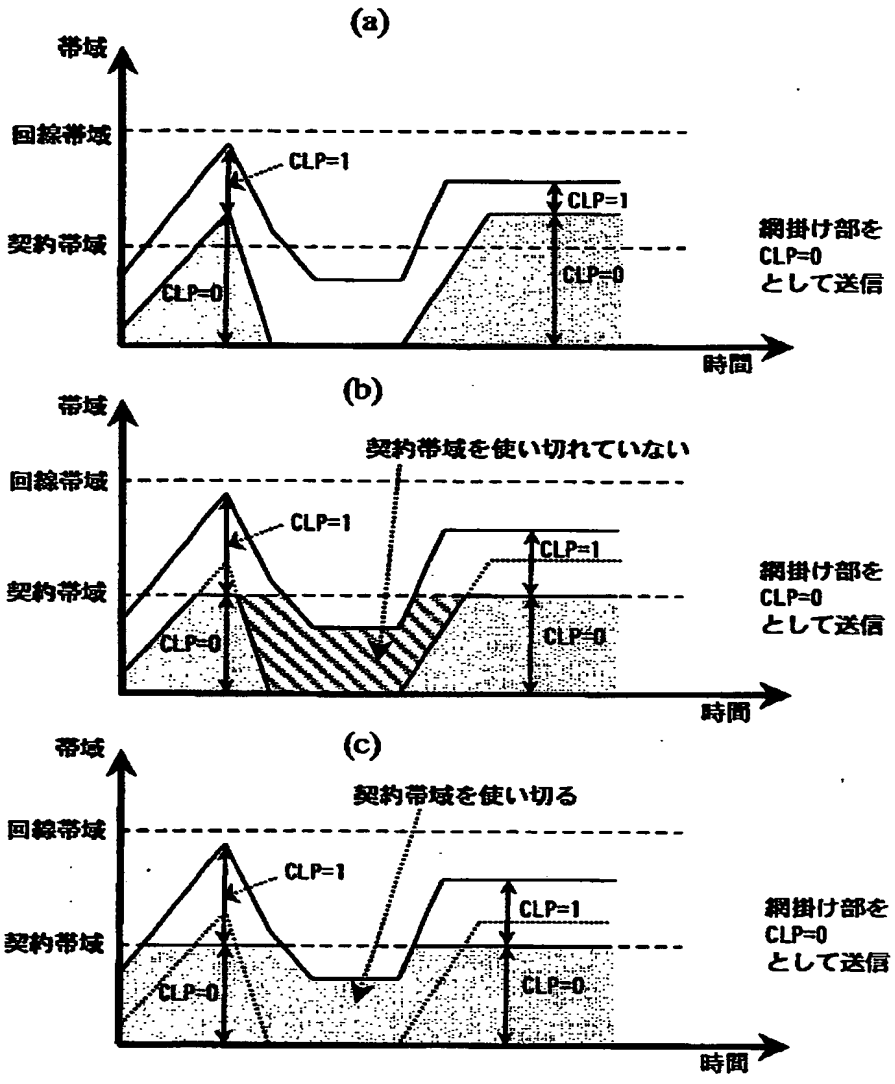
【図１４】

図14


1441
帯域監視部
DSCPC
蓄積手段
532
DSCP判定部
DSCP
判定回路
531
530
12
パケット
受信回路160へ
DSCPN
蓄積手段
533
15
監視結果判定部
1421
1320
THR
蓄積手段
523
監視結果
判定回路
16
1422
コネクション
優先度
蓄積手段
1424
パケット長
蓄積手段
19
18
パケット
受信回路160より
コネクション
優先度判定部
1440
パケツ蓄積量判定部
POLR
蓄積手段
513
パケツ蓄積量
判定回路
TS
蓄積手段
514
511
CNT
蓄積手段
512
タイマー
515
550
510
帯域監視
テーブル
帯域監視テーブル
制御回路
1460
1461
帯域監視テーブル制御部

【図１５】

図15


(a)
帯域
回線帯域
契約帯域
CLP=1
CLP=0
CLP=1
CLP=0
網掛け部を
CLP=0
として送信
時間
(b)
帯域
契約帯域を使い切れていない
回線帯域
契約帯域
CLP=1
CLP=0
CLP=1
CLP=0
網掛け部を
CLP=0
として送信
時間
(c)
帯域
契約帯域を使い切る
回線帯域
契約帯域
CLP=1
CLP=0
CLP=1
CLP=0
網掛け部を
CLP=0
として送信
時間

【書類名】　要約書

【要約】

【課題】　優先パケットを非優先パケットよりも優先的に転送する網において、網利用者と網運用者間で優先パケットの帯域が契約されており前記網の入口の帯域監視装置にて前記優先パケットの帯域を監視する時、網利用者が送出する優先パケットが契約帯域未満の時には網利用者は契約帯域を十分利用できない。

【解決手段】　帯域監視装置の帯域監視部141において、監視結果判定部520が優先パケットの帯域が契約帯域未満であることを検出した場合、DSCP判定部530が非優先パケットを優先パケットと判定する。すなわち、網は、非優先パケットを優先パケットとして送信する。

【効果】　網利用者が契約帯域を十分利用できる。

【選択図】　図5

出　願　人　履　歴　情　報

識別番号　　〔０００００５１０８〕

１．変更年月日　　１９９０年　８月３１日
［変更理由］　新規登録
住　所　東京都千代田区神田駿河台４丁目６番地
氏　名　株式会社日立製作所